BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/80149 A2

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US01/40552

(22) International Filing Date: 18 April 2001 (18.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/551,309 18 April 2000 (18.04.2000) US

(71) Applicant: WAYPORT, INC. [US/US]; Suite A-300, 8303 North MoPac Expressway, Austin, TX 78759 (US).

(72) Inventors: STEWART, Brett, B.; P.O. Box 50544, Austin, TX 78763-0544 (US). THOMPSON, James, W.; 4417 Ridge Oak Drive, Austin, TX 78731 (US).

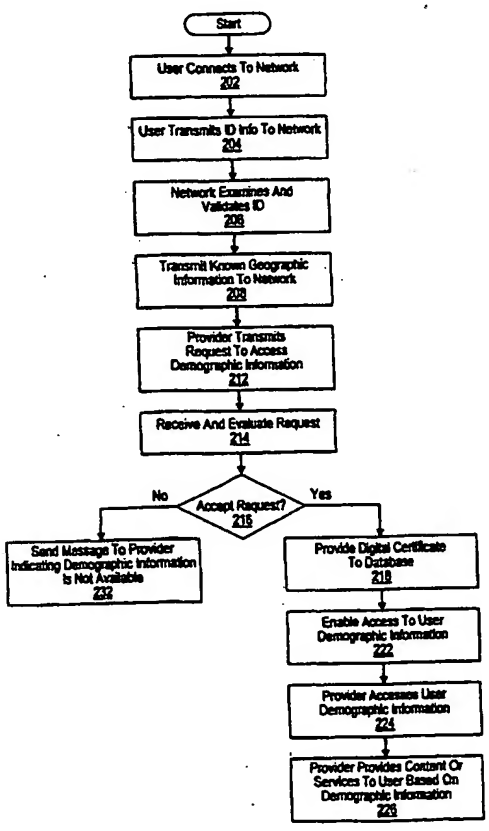
(74) Agent: HOOD, Jeffrey, C.; Conley, Rose & Tayon, P.C., P.O. Box 398, Austin, TX 78767-0398 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR MANAGING USER DEMOGRAPHIC INFORMATION USING DIGITAL CERTIFICATES



(57) Abstract: A system and method for enabling users to more efficiently manage and control user demographic data in an information network, such as the Internet, including provision of infomediary services. The system may comprise a network, wherein a plurality of providers, such as information providers and service providers, may be coupled to the network. One or more databases may also be coupled to the network which include demographic information of various users. Users may operate computing devices to access the network for information and services. The demographic information stored in databases on the network is not usable or accessible by third parties for providing information to the various users. Each of the computing devices operated by various users may include a digital certificate which may store access information for enabling use of the respective user's demographic information. Thus, a user may use the stored digital certificate to manage access to the user's demographic data stored in the database. A user may selectively provide a digital certificate to the database, or a provider, to selectively allow access to the respective user's demographic data.

WO 01/80149 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE: SYSTEM AND METHOD FOR MANAGING USER DEMOGRAPHIC INFORMATION USING DIGITAL CERTIFICATES

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to network communications, and more specifically to the management of user demographic information, such as the provision of infomediary services, using digital certificates and concepts of paired key cryptology.

2. Description of the Relevant Art

Electronic commerce or Internet commerce has become an increasingly popular form of commerce in the United States and throughout the world. In general, electronic commerce or Internet-based commerce, often referred to as e-commerce, provides vendors and service providers the ability to greatly increase their sales channel and distribution network with minimal cost. An electronic commerce site provides a convenient and effective mechanism for potential customers to use, select and purchase products in an easy and simple fashion.

The Internet has dramatically changed many types of business practices and business models. Many businesses attempt to capture customer information and use this information for commercial purposes. For example, various businesses operate to track, record and sell customer information for personal gain, including personal data about customers such as buying habits, income levels, credit card usage etc. The result to consumers is typically large amounts of unwanted junk mail, unwelcome advertising and solicitations. A relatively new concept in Internet business models is referred to as an "infomediary" (information intermediary). An infomediary can be defined as a business or company which helps customers to capture and maximize the value of their personal demographic information, possibly allowing customers to manage their personal data for financial benefit. In order to support the business model of an infomediary, new methods are desired for enabling customer demographic data to be tracked and recorded while still allowing customers management and control over this data, including the ability of customers to selectively decide whether to release this data to third parties.

In general, it would be very desirable to provide customers or users with an improved mechanism for managing and controlling their personal customer data, while still allowing selective access to this data by various third party providers.

Background on digital certificates is deemed appropriate. Digital certificates are a very useful tool for Internet transactions. A digital certificate may reside in a client computer and may be used to identify the client computer. In general, digital certificates are used to authenticate users and perform secure transactions. When a client or user accesses a web site, the client computer may transmit its digital certificate to the web server. Without the use of digital certificates, user access to a web site may require registration and the use of passwords by users accessing the site, which is generally inconvenient. For example, a user typically receives different passwords and user ID information from different providers, and users may often times forget their individual passwords and IDs. Thus, digital certificates solve many of the problems associated with requiring registration and the use of passwords.

Therefore, digital certificates are useful for performing secure electronic commerce (e-commerce) transactions, and may be used to uniquely identify users. This unique identification may allow an Internet-based business gather information about customers in order to customize their access to a given web site. For example, the use of digital certificates allows a web site to restrict access, including the ability to allow different users different levels of access. A digital certificate may also allow for the instant authentication of a user without requiring the use of a user name or password.

Digital certificates utilize an encryption technology known as public/private key technology. A key is a unique encryption device, and no two keys are the same. This allows a given key to be used to identify its owner. Keys function in pairs, where one key within the pair is referred to as the public key, while the other key is referred to as the private key. A user thus has both a public key and a private key. The user may provide his public key to various trusted entities, but keeps the private key secure. Thus, public keys may be distributed freely to any end user who wishes to conduct secure transactions with the distributing user or web site, while a private key may be stored exclusively on a computer or server of the distributing user or web site. Each user also maintains a list of public keys of other users for use in sending encrypted email. When a third party desired to send an encrypted message to a recipient, the third party first must have that recipient's public key. The third party uses the recipient's public key to encrypt the message, and provides the encrypted message to the recipient. The recipient of the message then uses his private key to decrypt the message. Thus the public key of a user may encrypt information to be transmitted across the Internet to the user, and only the corresponding private key of the user may decrypt this information. Alternatively, a private key may encrypt information to be transmitted across the Internet, and only the corresponding public key may decrypt this information.

When a digital certificate is installed on the client computer of the end user, the digital certificate stores non-mutable or non-changeable information from the provider. If a server computer wishes to exchange information with the client computer of an end user, the server computer may access the digital certificate stored on the client computer, which contains the information from the certificate provider. The server computer uses its public key to ensure the contents of the certificate are valid and un-modified, and may also validate the identity of the end user and to encrypt the information to be shared. Encryption may be accomplished using Secure Sockets Layer (SSL) technology.

Digital certificates are particularly useful for providing access to network services in subscriber based services. Subscriber based services may include Internet service providers, online services, and other types of information or service providers.

SUMMARY OF THE INVENTION

One embodiment of the present invention comprises an improved system and method for enabling users to more efficiently manage and control user demographic data in an information network, such as the Internet. The present invention may also comprise an improved system and method for providing infomediary services.

The system may comprise a network, wherein a plurality of providers, such as information providers and service providers, may be coupled to the network. The network may be a wired network, a wireless network, or a combination. One or more databases may also be coupled to the network which include demographic information of various users, such as one or more of identity information, contact information, profile information, sponsorship

information, class transaction information, purchasing habits, credit card usage, preferences and past activities. among others. Users may operate computing devices, e.g., computers, personal digital assistants, etc., to access the network for information and services.

In the preferred embodiment, the demographic information stored in the one or more databases on the network is not usable or accessible by third parties for providing information to the various users. Preferably, each of the computing devices operated by various users includes a digital certificate which may store access information for enabling use of the respective user's demographic information. Thus, a user may use the stored digital certificate to manage access to the user's demographic data stored in the database. For example, the users' computing device may present the respective user's digital certificate to the database to enable use of the user's demographic information by third party providers. As another example, in one embodiment the user may provide his/her respective digital certificate to a provider coupled to the network. When the provider receives the digital certificate the provider may then present the digital certificate to the database to enable access and use of the respective user's demographic information, e.g., for targeted advertising etc.

In one embodiment, the user demographic information stored on the database is intelligible and accessible to third-party providers, but no user association is maintained with respect to the demographic information. Thus the providers can access and use the demographic information, without knowledge of the identities of the users. In this embodiment, the digital certificate may store identify information and other access information and operates to associate the respective user of the digital certificate with his/her corresponding demographic information. Thus, presentation of the digital certificate to the database operates to associate the user with his respective demographic information. This embodiment may allow third-party providers to provide various targeted information or services to users, wherein the demographic information of the users is known, but the specific identities of respective users is unknown to the provider. As one example, if the user chooses to respond to a provider's offer or accept information from the user, the user can then provide his/her digital certificate in response to acceptance of the offer, e.g., to purchase an advertised product. As mentioned above, provision of the digital certificate allows the user's identity to be associated with the user's demographic information

In another embodiment, the user demographic information stored in the database is unintelligible or encrypted. In this embodiment, each user's digital certificate may include access information, such as a decryption key, password or other mechanism, which operates to render the respective user's demographic information intelligible. For example, the demographic information stored in the database may be encrypted using a first key, e.g., a public key, and the digital certificate may include a second key, e.g., a private key wherein this private key is required to decrypt the respective user's demographic information. Thus, in this embodiment, the demographic information stored in the database is unintelligible to providers, and the user first presents his/her digital certificate to the database, or to a provider, to render the demographic information intelligible and hence useful by a third-party provider. This provides the user with greater control over his/her demographic data. In this embodiment, the identity of the user may become known to the provider when the user presents his/her digital certificate. Alternatively, the identity of the user may still remain anonymous, wherein the access information or key stored in the digital certificate merely allows a provider to discover the demographic information of the user, possibly without discovering the identity of the user who is associated with this demographic information. This would allow

the providers, at the user's discretion, to provide targeted information or services to users who are essentially anonymous to the provider.

In another embodiment, the digital certificate itself may store a portion of the user's demographic data, such as sponsorship information, including information regarding programs or entities in which the mobile user is a member or is affiliated. In yet another embodiment, the digital certificate may be configured to selectively allow different levels of access to the user's demographic information, e.g., depending on the trust level ascribed to the provider. In this embodiment, the demographic information or the access level information may be stored in extensions within the digital certificate.

Therefore, the system and method described herein operates to provide users and customers with greater control and access over their customer data or demographic information. Thus, each user's demographic information is stored and maintained on the database, perhaps by an infomediary, and this information is possibly not usable, not accessible, or unintelligible, by third-party providers without the user providing express permission for transfer of the digital certificate stored on the respective user's computing device. This allows use of user demographic information by various third-party providers while providing control or management of this information by the respective users.

In one embodiment, the user is a mobile user (MU), also referred to as a subscriber, who may access the network service through a portable computing device (PCD) using a wireless (or wired) network interface card. Access points (APs) for the network may be widely distributed in various facilities, such as airports, mass-transit stations, and various businesses, such as coffee shops or restaurants at an airport. When in sufficiently close range to an access point, the PCD may access the service through the network card. In one embodiment, the APs are arranged at known geographic locations and may provide geographic location information regarding the geographic location of the mobile user (MU). A digital certificate may be stored on the mobile user's PCD. When accessing the network, the digital certificate may be selectively provided by the user to selectively enable access by providers to the user's demographic information stored on the network, or other information such as billing/charging information.

BRIEF DESCRIPTION OF THE DRAWINGS

Other objects and advantages of the invention will become apparent upon reading the following detailed description and upon reference to the accompanying drawings in which:

Figure 1 is a block diagram of one embodiment of a network system incorporating the present invention;

Figure 1A is a block diagram of one embodiment of a wireless network communication system incorporating the present invention;

Figure 2 is a block diagram of one embodiment of a computer system of a provider; and

Figure 3 is a flowchart diagram of one embodiment of a method of allowing access to demographic information in a network using an improved infomediary model.

While the invention is susceptible to various modifications and alternative forms, specific embodiments thereof are shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that the drawings and detailed description thereto are not intended to limit the invention to

the particular form disclosed, but on the contrary, the intention is to cover all modifications, equivalents and alternatives falling within the spirit and scope of the present invention as defined by the appended claims.

DETAILED DESCRIPTION OF THE EMBODIMENTS

Incorporation by Reference

U.S. Patent No. 5,835,061, titled "Method and Apparatus for Geographic-Based Communications Service", whose inventor is Brett B. Stewart, is hereby incorporated by reference in its entirety as though fully and completely set forth herein.

U.S. Patent Application Serial No. 09/433,817 titled "Geographic Based Communications Service" and filed on November 3, 1999, whose inventors are Brett B. Stewart and James Thompson, is hereby incorporated by reference in its entirety as though fully and completely set forth herein.

U.S. Patent Application Serial No. 09/433,818 titled "A Network Communications Service with an Improved Subscriber Model Using Digital Certificates" and filed on November 3, 1999, whose inventors are Brett B. Stewart and James Thompson, is hereby incorporated by reference in its entirety as though fully and completely set forth herein.

Figure 1 – Exemplary Network Communication System

Figure 1 illustrates a simplified and exemplary network system according to one embodiment of the present invention. The network system may be used for general information access and/or electronic commerce (e-commerce) or Internet commerce. The embodiment illustrated in Figure 1 includes one provider server 102, one database server 108 and one client system 106, which each may be coupled to a network 104 such as the Internet. However, it is noted that the present invention may be utilized with respect to any number of provider servers 102, database servers 108 and client systems 106.

As shown in Figure 1, the provider who maintains the provider server 102 may offer one or more of information, content or products over network 104, such as the Internet. For example, the provider may offer advertising content, such as targeted advertising, to clients over the network 104. The provider may also be a vendor who offers products, for sale over network 104, such as the Internet, and preferably maintains the provider server 102 as an e-commerce server 102. One example of an e-commerce vendor is Amazon.com, which sells books and other items over the Internet. In general, the provider may offer any of various types of goods or services over the network 104, wherein services offered include any of various types of information or content, as well as services such as financial services, etc.

As shown, the provider server 102 may be connected to a network 104, preferably the Internet 104. The Internet 104 is currently the primary mechanism for performing electronic commerce. However, the network 104 may be any of various types of wide-area networks, local area networks, or networks of networks, such as the Internet, which connects computers and networks of computers together. Thus, the network 104 may be any of various types of networks, including wired and wireless networks, or combinations thereof. The network 104 may include or be coupled to other types of communications networks, (e.g., other than the Internet) such as the public switched telephone network (PSTN), among others.

As shown, the database server 108 may also be connected to the network 104. The database server 108 may be maintained by a provider, or by a third party "infomediary". The database server 108 may store demographic information for a plurality of different users. In the preferred embodiment, the demographic information of a first user stored on the database server 108 is not useable by a provider for providing information (e.g., content) to the first user without a digital certificate provided from the first user. Alternatively, or in addition, the demographic information of a first user stored on the database server 108 is not associable to the first user without a digital certificate provided from the first user. Alternatively, or in addition, the demographic information of a first user comprised in the database is unintelligible, e.g., is encrypted, and the digital certificate provided from the first user is necessary to decrypt this information.

As noted above, the database server 108 may be operated or maintained by a third party, which may be referred to as an "infomediary". The party who maintains the database server 108 may collect and store demographic information on users, such as past transactions and commercial activities of the users, and other types of demographic information. The demographic information is stored on the database server 108, and, as mentioned above, the user preferably maintains at least some control and management of his/her demographic information. The infomediary may receive a financial benefit from a provider 102 when the infomediary provides demographic information to the provider. The user may also receive a financial benefit when the user chooses to allow a provider access to his/her demographic information.

As used herein, the term "demographic information" includes one or more of identity information, contact information, profile information, sponsorship information, past transaction information, purchasing habits, credit card usage, restaurant or hotel preferences, rental car preferences, past activities, and past commercial activities, among other types of customer or user data. The term "profile information" includes one or more of age, weight, income level, residence location, and travel history, among other types of information. The term "sponsorship information" includes one or more of information regarding memberships of the user, information regarding incentive programs in which the user is a member, and information regarding entities in which the user is affiliated, among others. Thus, sponsorship information may include information regarding frequent flier program memberships (e.g., the American Airlines Advantage Program), rental car incentive programs (e.g., Hertz Number One Club Gold), bank affiliations, country club affiliations, and other programs or affiliations, such as other incentive programs, preferred status memberships, other programs sponsored by vendors of goods or services, and other organizations of which the user is affiliated. The demographic information thus may take any of various forms.

Client system 106 may also be connected to the network 104. The client system 106 is also referred to herein as a "computing device". The client system or computing device 106 may be of various kinds of systems such as a computer system, a network appliance, an Internet appliance, a Personal Digital Assistant (PDA), WebTV, telephone, two way pager, etc. The client system 106 may execute web browser software for allowing a user of the client system 106 to browse and/or search the Internet 104, as well as enabling the user to conduct transactions or commerce and/or receive information or content over the Internet 104. The web browser software in client computer system 106 may optionally utilize a 64-bit or 128-bit encryption technology to securely communicate with the provider server 102. When the user of the client system 106 desires to access a site, such as

a site of the provider server 102 over the Internet 104, the web browser software preferably accesses the Web site of the respective provider server 102.

The client system 106 of a first user may store a digital certificate which is used in managing or controlling access to the first user's demographic information comprised in the network, e.g., stored in the database 108. In one embodiment, the digital certificate stored on the client system 106 of the first user includes access information for enabling access to or use of the first demographic information by a provider, e.g., in providing information or content to the user. The digital certificate may also include an identity of the user, as well as other information. For example, the digital certificate may comprise a portion of the user's demographic information, such as sponsorship information, or may comprise charging and network usage information. In this embodiment, access charges for access to the network may be computed based on information, such as charging information and/or sponsorship information, comprised in the user's digital certificate. As used herein, the term "digital certificate" is intended to encompass any of various types of data structures which are used for gaining access to network resources.

The computing device 106 may be operable to present its digital certificate to the database server 108 or to the provider 102, wherein the user's provision of the digital certificate may enable one or more uses of the demographic information of the user comprised in the database 108. For example, the user's provision of the digital certificate may enable a provider to provide targeted content or information, e.g., advertising or inducements, to the computing device 106 of the user. The user's provision of his/her digital certificate may also or instead operate to associate the user with the corresponding demographic information and/or render the demographic information intelligible, e.g., decrypted.

Thus, in one embodiment, the demographic information of a user is not associable to the user without the first digital certificate, and the respective user's digital certificate comprises access information for associating the user with his/her demographic information. Thus the user's provision of his/her digital certificate may also or instead operate to associate the user with his/her corresponding demographic information.

In another embodiment, the demographic information of a user comprised in the database is unintelligible, e.g., is encrypted, and the digital certificate of the respective user contains the "key" necessary to decrypt the demographic information. Thus, presentation of the respective user's digital certificate to the database 108 renders the user's demographic information intelligible or unencrypted. For example, the demographic information of a user comprised in the database may be encrypted using a first key, and the digital certificate of the respective user may include a second key, wherein the second key from the user's digital certificate is used to decrypt the user's demographic information.

The computing device 106 may present the digital certificate directly to the database server 108. Alternatively, the provider server 102 may receive the digital certificate from the computing device 106 and then present the digital certificate to the database server 108. As noted above, presentation of the digital certificate to the database server 108 may enable use of or access to the demographic information of the user comprised in the database server 108.

As noted above, a user's digital certificate may comprise access information for enabling use of or access to the user's demographic information. and provision of the digital certificate enables use of or access to the

demographic information of the user comprised in the database. In one embodiment, the user may receives some type of financial benefit in return for provision of the first digital certificate.

The provider may take various actions in response to gaining access to the user's demographic information. For example, the provider server 102 may provide information or content to the user based on the demographic information. The provider server 102 may use the demographic information to select or generate targeted advertising, inducements, offers, etc. to the user.

Database Server 108, Provider Server 102 and Client System 106

The database server 108, the provider server 102, and the client system 106 may each include various standard components such as one or more processors or central processing units, one or more memory media, and other standard components, e.g., a display device, input devices, a power supply or batteries, etc. The provider server 102 and the database server 108 may also each be implemented as two or more different computer systems.

One or more of the database server 108, the provider server 102, and/or the client system 106 may each include a memory medium on which computer programs or data (e.g., a digital certificate) according to the present invention may be stored. The term "memory medium" is intended to include various types of memory or storage, including an installation medium, e.g., a CD-ROM, or floppy disks, a computer system memory, e.g., random access memory (RAM), such as DRAM, SRAM, EDO RAM, Rambus RAM, etc., or a non-volatile memory such as a magnetic media, e.g., a hard drive, or optical storage. The memory medium may comprise other types of memory as well, or combinations thereof. In addition, the memory medium may be located in a first computer in which the programs are executed, or may be located in a second different computer which connects to the first computer over a network. In the latter instance, the second computer provides the program instructions to the first computer for execution. Also, the servers 102 and/or 108 may take various forms, including a computer system, mainframe computer system, workstation, or other device. In general, the term "computer system" or "server" can be broadly defined to encompass any device having a processor that executes instructions from a memory medium.

The memory mediums on each of the database server 108, the provider server 102, and/or the client system 106 may store software or data to enable users to manage and/or control their demographic information in a network system according to the methods or flowcharts described below. The software programs may be implemented in any of various ways. Also, the digital certificate may have any of various forms. A CPU, such as the host CPU, executing code and data from a memory medium comprises a means for implementing the network system described herein.

Various embodiments further include receiving or storing instructions and/or data implemented in accordance with the foregoing description upon a carrier medium. Suitable carrier media include memory media or storage media such as magnetic or optical media, e.g., disk or CD-ROM, as well as signals such as electrical, electromagnetic, or digital signals, conveyed via a communication medium such as networks and/or a wireless link.

Figure 1A - Wireless Network Communication System

Figure 1A shows one embodiment of an exemplary wireless network communication system 100A. The wireless network communication system 100A may include a portable computing device (PCD) 106A with a wireless connection 111 (e.g., an antenna) in communication with a wireless access point (AP) 120 having a

wireless connection 121 (e.g., an antenna). The AP 120 may be coupled to a provider 102 and a management information base (MIB) 150 through network 104. The network 104 may comprise a wired network, a wireless network or a combination of wired and wireless networks.

The network communication system 100A may be geographic-based. In other words, the network communication system 100A may provide information and/or services to the MU based at least partly on the known geographic location of the MU, e.g., as indicated by the access points 120 or as indicated by geographic information (e.g., GPS information) provided from the PCD 106A.

The wireless communication system 100A may include a plurality of wireless access points 120, a plurality of providers 102, and/or a plurality of MIBs 150. Access points (APs) for the network may be widely distributed in various facilities, such as airports, mass-transit stations, shopping malls, and other businesses, such as coffee shops or restaurants at an airport. When in sufficiently close range to an access point, the PCD 106A may access the network through, for example, a wireless network card. In one embodiment, the APs 120 are arranged at known geographic locations and may provide geographic location information regarding the geographic location of the mobile user (MU) or the PCD 106A. In another embodiment, the PCD 106A may provide geographic location information of the PCD 106A through the AP 120 to the network 130. For example, the PCD 106A may include GPS (Global Positioning System) equipment to enable the PCD 106A to provide its geographic location through the AP 120 to the network 130, e.g., service provider 140 located on the network 130.

The service providers 140 and MIBs 150 each may comprise a computer system coupled to the network 130. The network 130 may comprise one or more wired or wireless local area networks and/or one or more wide area networks (e.g., the Internet). Each service provider 102 may include one or more computers or computer systems configured to provide goods, information, and/or services as appropriate for the service provider. The one or more service providers 102 may connect to network 104 in a wired or wireless fashion. The one or more MIBs 150 may be comprised in a provider 102.

The wireless communication may be accomplished in a number of ways. In a preferred embodiment, PCD 106A and wireless AP 120 are both equipped with an appropriate transmitter and receiver compatible in power and frequency range (e.g., 2.4GHz) to establish a wireless communication link (e.g., wireless connection 111 and wireless connection 121, respectively). Wireless communication may also be accomplished through cellular, digital, or infrared communication technologies, among others. To provide user identification and/or ensure security, the MU may also be equipped with a code generator that generates an identification code that may be transmitted to and recognized by the wireless AP 120. This identification code may then be relayed to different service providers 102 and/or MIB 150 that are coupled to wireless AP 120 via network 104. Such an identification code may utilize recognition of a MU before providing access to system services, thereby providing a measure of security and a service billing mechanism. As described above, the PCD 106A may selectively provide a digital certificate or other data to selectively enable a provider 102 to use or access demographic information of the user. In one embodiment, the demographic information of the user may be used in conjunction with the known geographic location of the user to provide specific or targeted information (e.g., advertising) to the user.

In various other embodiments, the system 100 may be a wired network communication system or a hybrid (wired and wireless) network communication system. For more information on possible embodiments of the system, including various embodiments of the access points 120 and the PCD 106A, please see U.S. Patent Nos.

5,835,061 and 5,969,678, and U.S. patent application Serial No. 09/433,817, which are hereby incorporated by reference as though fully and completely set forth herein.

Computing Device 106

As noted above, the computing device or client system 106 may be any of various types of devices, including a computer system, such as a portable computer, a personal digital assistant (PDA), an Internet appliance, a communications device, such as a cellular phone, digital wireless telephone, or other wired or wireless device. The computing device 106 may include various wireless or wired communication devices, such as a wireless Ethernet card, cellular telephone logic, paging logic, RF communication logic, a wired Ethernet card, a modem, a DSL device, an ISDN device, an ATM device, a parallel or serial port interface, or other type of communication device. As mentioned above, the computing device 106 preferably includes a memory medium which stores a digital certificate. The digital certificate may also be referred to as a personal certificate. The digital certificate may be stored in a web browser of the personal computing device 110.

The digital certificate may comprise a reference or cookie to the user's demographic information, which may be kept on a separate server, e.g., the database server 108. The references or cookies may take the form of a URL, a pointer, an IP address, or other reference or cookie.

The digital certificate stored on the client system or computing device 106 includes access information for rendering the respective user's demographic information useable, accessible, or intelligible. The access information may be stored in extensions within the digital certificate, such as non-critical extensions. The access information may take any of various forms. Where the demographic information is stored in an encrypted format on the database server 108, the access information may comprise a "key" or other data for decrypting the information. In general, the access information may comprise some type of data which may operate to effectively "unlock" the demographic information or make the demographic information useable or accessible in some way.

The digital certificate may also store various other information, such as charging information of the user or sponsorship information of the user. The sponsorship information and/or charging information may also be stored in extensions within the digital certificate, such as non-critical extensions of the digital certificate.

Figure 2 - Database Server Service Provider

Figure 2 is an exemplary block diagram of one embodiment of a database server 108. The database server 108 may take any of various forms, and Figure 2 is exemplary only. The database server 108 may comprise a processor 310 coupled to a system bus 330. Processor 310 may be any of several different processors. A database 325 and memory 320 may also be coupled to the system bus 330. The database 325 preferably stores user demographic information of a plurality of users. System bus 330 may be coupled to I/O bus 335. Network interface 340 may also be coupled to I/O bus 335. System bus 330 and I/O bus 335 may be coupled to other devices, such as a display.

The demographic information of the plurality of users is preferably stored in a manner where the demographic information of a user is not useable or accessible to providers without being paired with the corresponding user's digital certificate. This allows each user a manner of control or management of his/her respective demographic information. In one embodiment, the demographic information is stored in an encrytped

format, and the digital certificate from the corresponding user is required to decrypt the demographic information. In another embodiment, the demographic information is stored in a normal readable format. However, the database server 108 may be configured to provide the demographic information of a user in an encrypted or unintelligible format unless the user's digital certificate has been provided.

Database server 108 may be operable to receive a digital certificate from a client system 106 of a user and extract various information from the digital certificate, such as a user identification and the access information. The access information may then be used for enabling access to the user's demographic information. The database 325 may store various types of information, such as demographic information of users, charging information of users, and/or other information. The digital certificate may make this other information accessible as well.

Thus the database 325 may store user demographic information that may only be available to registered network users or registered network providers using an access code or access information that has been approved by the user. Alternatively, the database 325 may selectively store user information, based on a permission received from the respective user. This information may be selectively provided by the database 325, upon the approval of the user as indicated by provision of a digital certificate of the user. Thus the database server 325 may act as an infomediary for users.

The processor 310 may use this access information in the digital certificate to access the respective user's demographic information from the database 325. The processor 310 may also access other information from the database 325, such as charging or usage information. This demographic information may be used by a provider, possibly in conjunction with geographic location information of the client system 106, to provide targeted services or information (e.g., advertising information) to the user. The provider computer 102 may receive information or service requests from network 104, determine what information fulfills each request, and make the information available to the user over the network 104.

The database server 108 may also store charging information used for charging the user for network access. The charging information may include information regarding participation in various incentive programs which may affect network access charging, e.g., programs which offer a limited time period of free or reduced charge network access. The charging information may also include information regarding an amount of available network access usage, e.g., a time amount, a dollar amount, or an amount of accrued "points". For example, the amount of "points" may indicate an amount of network usage available to the user.

Figure 3 - Demographic Information Management using the Improved Infomediary Model

Figure 3 is a flowchart diagram illustrating operation of allowing access to demographic information in a network using an improved infomediary model. In one embodiment, as described above, the client system or computing device 106 includes a digital certificate stored in the memory of the computing device 106. The digital certificate may store information need for user authentication and security on the network. The digital certificate may also store access information, as described above, for selectively allowing access to the user's demographic data. The digital certificate may also store references to other information, such as demographic information of the user, charging information of the user, or other information.

The network access method of the present invention may be operable to receive and use the digital certificate for authentication and security, as well as for enabling access to the user's demographic information. In

one embodiment, the system and method may extract and use information stored in the digital certificate, possibly in conjunction with geographic location information of the user and other information, to provide an improved infomediary service. Various providers on the network 104 may be allowed by the user to gain access to the user's demographic information, as indicated by the user's provision of his/her digital certificate. The providers may use this demographic information, possibly in conjunction with geographic location information of the user and/or other information, to provide various targeted services or information to the user.

As shown, in step 202 the user connects to the network 104 (e.g., to an access point of the network). For example, the user may connect to the Internet from his/her home or office. Where the user is a mobile user, the user may be walking in an airport with a portable computing device and may connect in a wireless fashion to an access point located at the airport. In another scenario, the user may enter a hotel room and connect to an Ethernet port in his/her room which is connected to the network. Thus, the user may connect to the network 104 in a wired or wireless fashion.

In step 204 the computing device 106 of the user may optionally transmit identification information (ID information) to the network or to the access point (AP) of the network. The identification information may take any of various forms. In one embodiment, the identification information comprises a digital certificate which contains various identification or authentication information. In another embodiment, the identification information comprises a MAC (media access controller) ID which is comprised on a wired or wireless Ethernet card of the personal computing device used by the user. In another embodiment, the identification information comprises an 802.11 (wireless Ethernet) System ID (SID). Thus, in one embodiment, the identification information may identify the user without "giving away" the user's identity (e.g., "anonymous identification"). In other words, the MAC ID or SID may be used to reference the proper demographic information, without indicating the actual identity or name of the user associated with this demographic information. The identification information may comprise other types of information, e.g., more secure identification, as desired.

In step 206 the network provider may examine and validate the received identification information, e.g., the certificate, MAC ID, the 802.11 System ID, or other identification information. The identification information may be accompanied by a password or other type of information. As noted above, the identification information may also be comprised in a digital certificate, which may be different than the digital certificate used to grant access to the user's demographic information.

Steps 204 and 206 may be performed where the user is connecting through a proprietary (third party) network 104 or through a proprietary portion of the network 104, or through an ISP. For example, steps 204 and 206 may be performed where the user is connecting through a proprietary portion of the network 104, e.g., where the user is a mobile user connecting to a proprietary wireless network for Internet access, or possible connecting through a third party ISP (Internet service provider).

In one embodiment, in step 208 geographic location information may be transmitted to the network. For example, where the user is a mobile user who connects to an access point 120, the access point 120 to which the user has connected may transmit known geographic location information to the network (e.g., an information provider on the network). Alternatively, the user's computing device 106 may transmit geographic location information using GPS technology or other means. As discussed further below, this known geographic location information of the user may be used to provide information or services to the user which are dependent upon the

geographic location of the user. For more information on the use of geographic location information for providing geographic based information and services, please see U.S. Patent No. 5,835,061, referenced above.

Once the user has connected to the network 104, e.g., the Internet, the user may perform various tasks as is well known. For example, the user may access various web sites to read or review various content such as travel information, weather information, stock market information, news or any of other various types of content. The user may also initiate purchase of various products, e.g., goods or services, available on electronic commerce sites, as is well known.

Various providers, either information providers or service providers, may desire to access the demographic information of various users for commercial purposes. For example, providers may desire access to users' demographic information to provide targeted advertising or inducements over the Internet or to provide various advertising mailings, etc. Thus, in step 212 a provider may transmit a request to access demographic information to a user.

In one embodiment, the provider may transmit the request directly to the user to ask the user whether the provider can access that respective user's demographic information. In this embodiment, in step 214 the user, i.e., the client system 106 of the user, may receive and evaluate the request. If the user decides to provide the requesting provider access to the user's demographic information in step 216, then in step 218 the client system 106 of the user may transmit its respective digital certificate to grant the requested access to the user's demographic information. Alternatively, the client system 106 may direct another computer to provide the digital certificate. In one embodiment, the user may provide the digital certificate to the provider, wherein the provider may then forward the digital certificate to the database 108 to gain access to the user's demographic information. In an alternate embodiment, the user or another computer may provide the digital certificate directly to the database 108, perhaps accompanied with or including a cookie or other reference to the respective provider whose request has been granted. As discussed in detail above, the provision of the digital certificate to the database 108 operates to enable access to or use of the respective user's demographic information.

In one embodiment, the user may provide the digital certificate with an access level or privilege level incorporated in the certificate, wherein this access level indicates the amount of the user's demographic information to which the provider may have access.

In step 222, in response to the digital certificate being provided to the database server 108, the provider may then access the user's demographic information and use this information for various purposes, such as providing targeted advertising inducements or offers to the user. For example, in step 224 the provider provides various content or services to the user based on the demographic information.

In one embodiment, a provider who gains access to a respective user's demographic information may then incorporate a preset or pre-determined discount to the user who granted the providers request, this discount forming an incentive to the user to grant access to the user's demographic information to the provider. The discount may also be based on the access level or privilege level provided in the user's digital certificate.

If the user decides to not provide access to the provider as determined in step 216, then in step 232 the client system 106 may provide a message to the provider indicating that the demographic information of the user is not available or accessible to that provider. The provider may then optionally provider a greater incentive or inducement to the user for the user to release his/her demographic information.

Alternate Embodiment

In an alternate embodiment of the invention, each of the users who have demographic information stored or collected on the database 108 may have previously transmitted their respective digital certificates to the respective infomediary who maintains the database 108, accompanied with directions or instructions as to when the respective user consents to a provider's request to access the demographic information. For example, respective users may require certain discounts or financial incentives from providers before they will grant access to this demographic information. Thus, in this embodiment, the database server 108 maintains user demographic information for a plurality of users, and maintains a corresponding digital certificate for each of the respective users, wherein the digital certificate contains the necessary access information for enabling access to or use of the user demographic information, and further the database 108 may maintain instructions from each of the respective users which specify criteria for granting access to the respective user's information to providers.

In this embodiment, in step 212 the provider transmits request access demographic information, wherein the request is made directly to the infomediary who maintains the database server 108. In step 214 the infomediary may receive and evaluate the request based on the user's previously specified instructions as to when to provide demographic information to providers. For example, the infomediary may retrieve the user's criteria for releasing this information such as types and/or kinds of providers, types of products offered, type and/or amount of discount offered, etc. In one embodiment, users may be treated as groups or classes, and the infomediary may selectively allow access to demographic information of respective groups or classes of users based on various criteria or financial incentives offered to the group or class of users. This may allow the infomediary to aggregate users, or allow the users to aggregate themselves, to negotiate higher discounts or greater incentives for access to their collective demographic information.

If the infomediary decides to allow access to the user's demographic information as determined in step 216 then in step 218 the infomediary may retrieve the digital certificate stored in its database or from the user's client system 106 and use the certificate to enable access to the demographic information in step 220. The provider may then access the demographic information of the user(s) in step 222.

If the infomediary determines to not provide access as determined in step 216, then in step 232 the infomediary provides a message to the provider indicating that the demographic information of the user is not available or accessible to that provider. The provider may then optionally provider a greater incentive or inducement to the user, or group of users, for the infomediary to release this demographic information. The infomediary may thus negotiate on behalf of the group of users to obtain the best discounts, incentives, or inducements to release demographic information of the users.

While the present invention has been described with reference to particular embodiments, it will be understood that the embodiments are illustrative and that the invention scope is not so limited. Any variations, modifications, additions, and improvements to the embodiments described are possible. These variations, modifications, additions, and improvements may fall within the scope of the inventions as detailed within the following claims.

WHAT IS CLAIMED IS:

1. A system, comprising:

a computing device operated by a user, wherein the computing device includes a first digital certificate;

a network;

wherein the computing device is operable to be coupled to the network; and

a database coupled to the network which stores first demographic information of the user;

wherein the first demographic information is not useable for providing information to the user without the first digital certificate.

2. The system of claim 1,

wherein the first digital certificate includes access information for enabling use of the first demographic information in providing information to the user.

3. The system of claim 1,

wherein the computing device is operable to present the first digital certificate to the database, wherein presentation of the first digital certificate to the database enables use of the first demographic information of the user comprised in the database.

4. The system of claim 1, further comprising:

at least one provider connected to the network, wherein the provider is operable to receive the digital certificate from the computing device, wherein the provider is operable to present the first digital certificate to the database, wherein presentation of the first digital certificate to the database enables use of the first demographic information of the user comprised in the database.

5. The system of claim 1, wherein the first demographic information in the database is not associable to the user without the first digital certificate;

wherein presentation of the first digital certificate to the database operates to associate the user with the first demographic information.

6. The system of claim 5,

wherein the first digital certificate comprises access information for associating the user with the first demographic information.

7. The system of claim 6, wherein the first digital certificate includes an identity of the user.

8. The system of claim 1, wherein the first demographic information comprised in the database is unintelligible without the first digital certificate;

wherein the first digital certificate comprises access information for rendering the first demographic information intelligible.

9. The system of claim 8,

wherein the first demographic information comprised in the database is encrypted using a first key;

wherein the first digital certificate includes a second key;

wherein the second key from the first digital certificate is used to decrypt the first demographic information.

10. The system of claim 1, wherein the first digital certificate comprises access information for enabling use of the first demographic information in providing information to the user;

wherein provision of the first digital certificate enables use of the first demographic information of the user comprised in the database;

wherein the user receives a financial benefit in return for provision of the first digital certificate.

11. The system of claim 1, wherein the demographic information includes one or more of identity information, contact information, profile information, sponsorship information, past transaction information, purchasing habits, credit card usage, restaurant or hotel preferences, rental car preferences, and past activities;

wherein profile information includes one or more of age, weight income level, residence location, and travel history;

wherein sponsorship information includes one or more of information regarding memberships of the mobile user, information regarding incentive programs in which the mobile user is a member, and information regarding entities in which the mobile user is affiliated.

12. The system of claim 1,

wherein the first digital certificate comprises sponsorship information;

wherein access charges for access to the network are computed based on the sponsorship information comprised in the first digital certificate.

13. The system of claim 1, further comprising:

at least one provider connected to the network, wherein the provider is operable to receive the first digital certificate from the computing device, wherein at least one provider is operable to access the first demographic information in the database using the first digital certificate and provide information to the user based on the first demographic information.

14. The system of claim 1, further comprising:

at least one provider connected to the network, wherein the provider is operable to receive the digital certificate from the computing device, wherein at least one provider is operable to access the demographic

information in the database using the first digital certificate and provide a service to the user based on the first demographic information..

15. The system of claim 1, wherein the computing device is a portable computing device operated by a mobile user; the system further comprising:

a plurality of access points connected to said network, wherein each of the plurality of access points is configured to detect the portable computing device.

16. The system of claim 1, wherein the computing device is a portable computing device operated by a mobile user;

wherein the portable computing device is configured to transmit a signal indicating a presence of the portable computing device

17. A system, comprising:

a computing device operated by a user, wherein the computing device includes a first digital certificate;

a network;

wherein the computing device is operable to be coupled to the network; and

a database coupled to the network which stores first demographic information of the user;

wherein the first demographic information is not associable to the user without the first digital certificate.

18. The system of claim 17, wherein presentation of the first digital certificate to the database operates to associate the user with the first demographic information.

19. The system of claim 17, wherein the first digital certificate comprises access information for associating the user with the first demographic information.

20. The system of claim 17, further comprising:

at least one provider connected to the network, wherein the provider is operable to examine the first demographic information in the database and provide information to the user based on the first demographic information, wherein the provider provides information to the user without knowledge of an identity of the user associated with the first demographic information.

21. A method for selectively providing access to demographic information of users in a network system, the method comprising:

storing a first digital certificate in a memory of a computing device operated by the user;

storing first demographic information of a user in a database, wherein the first demographic information in the database is not useable for providing information to the user without the first digital certificate;

transmitting the first digital certificate to the database, wherein the first digital certificate includes access information for enabling use of the first demographic information in providing information to the user; and

accessing the first demographic information after said transmitting.

22. The method of claim 21, wherein the network system includes at least one provider connected to the network;

wherein the provider performs said accessing the first demographic information;

the method further comprising the provider providing one or more of information or a service to the user based on the first demographic information.

23. The method of claim 23, wherein the network system includes at least one provider connected to the network;

wherein the provider performs said transmitting the first digital certificate to the database.

24. The method of claim 21, wherein the first demographic information in the database is not associable to the user without the first digital certificate;

wherein said transmitting the first digital certificate to the database operates to associate the user with the first demographic information.

25. The method of claim 24, wherein the first digital certificate comprises access information for associating the user with the first demographic information.

26. The method of claim 21, wherein the first demographic information comprised in the database is unintelligible without the first digital certificate;

wherein the first digital certificate comprises access information for rendering the first demographic information intelligible.

27. The method of claim 26,

wherein the first demographic information comprised in the database is encrypted using a first key;

wherein the first digital certificate includes a second key;

wherein the second key from the first digital certificate is used to decrypt the first demographic information.

28. The method of claim 21, wherein the user receives a financial benefit in return for said transmitting the first digital certificate.

29. The method of claim 21, wherein the demographic information includes one or more of identity information, contact information, profile information, sponsorship information, past transaction information, purchasing habits, credit card usage, restaurant or hotel preferences, rental car preferences, and past activities;

wherein profile information includes one or more of age, weight income level, residence location, and travel history;

wherein sponsorship information includes one or more of information regarding memberships of the mobile user, information regarding incentive programs in which the mobile user is a member, and information regarding entities in which the mobile user is affiliated.

30. A method for providing targeted information to a user in a network system, the method comprising:

storing a first digital certificate in a memory of a computing device operated by the user;

storing first demographic information of a user in a database, wherein the first demographic information in the database is not useable for providing information to the user without the first digital certificate;

transmitting the first digital certificate to the database, wherein the first digital certificate includes access information for enabling use of the first demographic information in providing information to the user;

accessing the first demographic information using the first digital certificate;

providing targeted information to the user using the first demographic information.

31. A computing device operated by a user on a network, comprising:

a processing unit;

a memory medium coupled to the processing unit including a first digital certificate, wherein the first digital certificate comprises access information for enabling use of first demographic information stored in the network;

a communication device for communicating with the network, wherein the communication device is also configured to transmit the first digital certificate;

wherein the first demographic information is not useable for providing information to the user without the first digital certificate.

32. A network system, comprising:

a database coupled to the network which stores first demographic information of a user;

at least one provider coupled to the network, wherein the provider is operable to receive a first digital certificate from a computing device operated by a user, wherein the first digital certificate comprises access information for enabling access to the first demographic information of the user stored in the database, wherein the at least one provider is operable to access the first demographic information of the user stored in the database in response to receiving the first digital certificate from the computing device operated by the user;

wherein the first demographic information is not useable by the provider without the first digital certificate.

33. The network system of claim 32, further comprising:

a plurality of access points coupled to the network, wherein each of the plurality of access points is configured to detect a computing device operated by a mobile user;

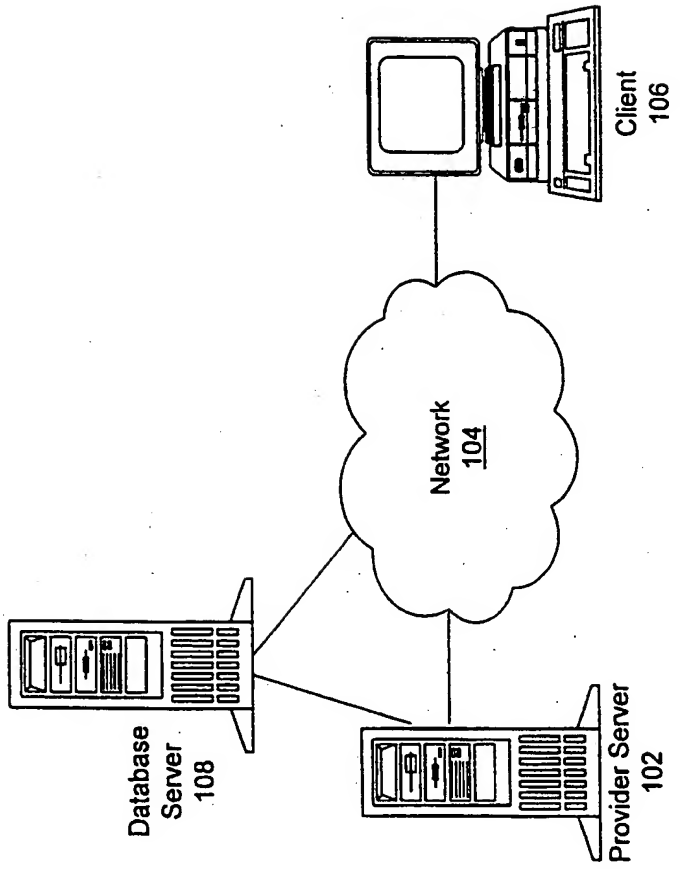

Client
106
Network
104
Database
Server
108
Provider Server
102

FIG. 1

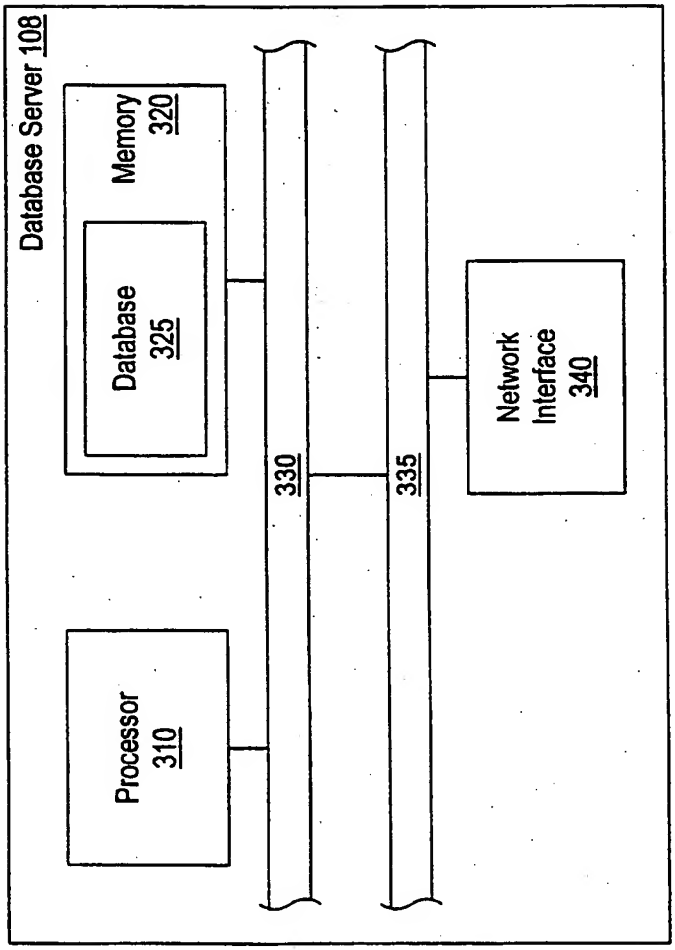

Database Server 108
Memory 320
Database 325
Processor 310
330
335
Network Interface 340

FIG. 2

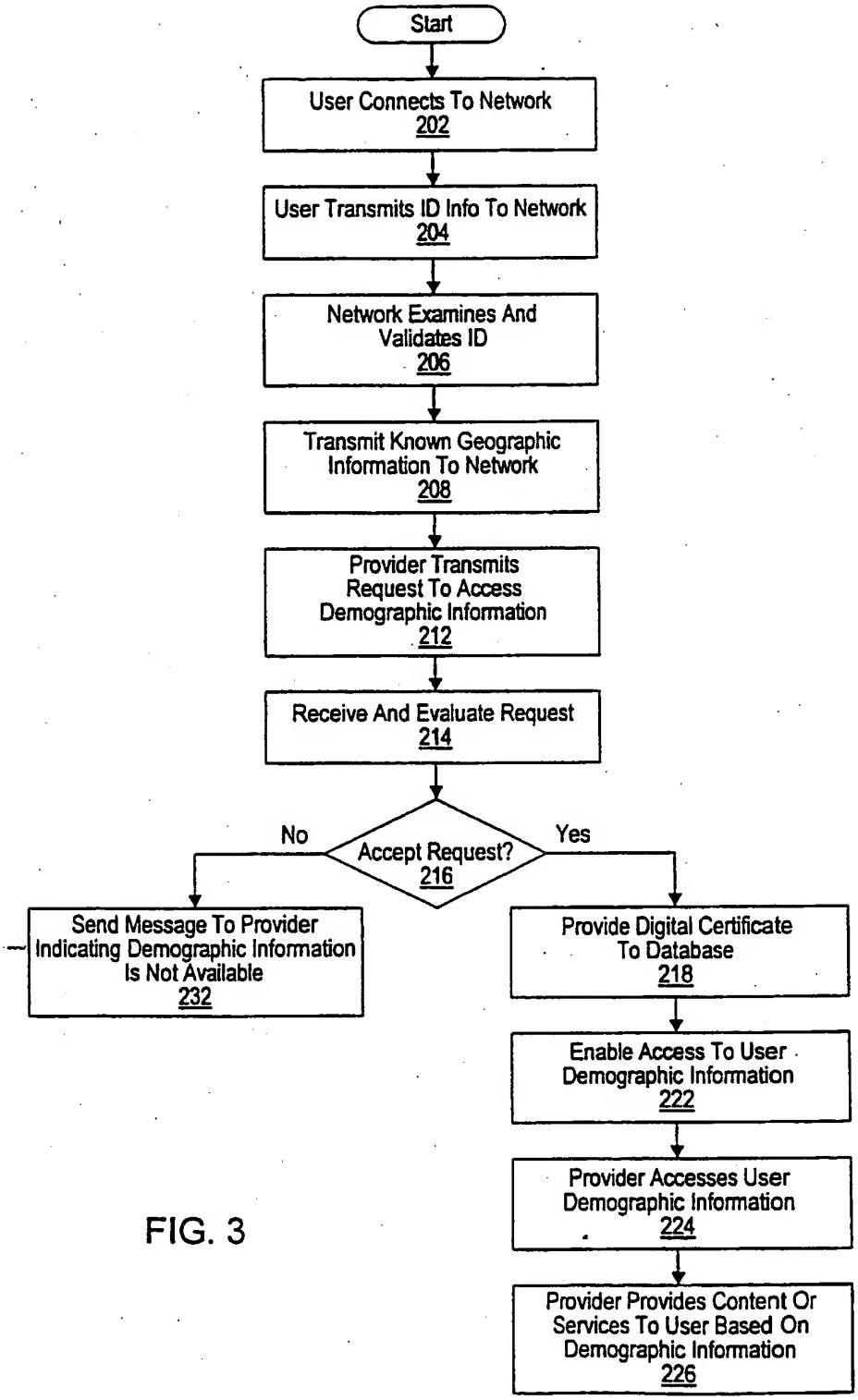

Start
User Connects To Network
202
User Transmits ID Info To Network
204
Network Examines And Validates ID
206
Transmit Known Geographic Information To Network
208
Provider Transmits Request To Access Demographic Information
212
Receive And Evaluate Request
214
Accept Request?
216
No
Yes
Send Message To Provider Indicating Demographic Information Is Not Available
232
Provide Digital Certificate To Database
218
Enable Access To User Demographic Information
222
Provider Accesses User Demographic Information
224
Provider Provides Content Or Services To User Based On Demographic Information
226

FIG. 3